REMARKS

The application includes claims 1, 2, 4-6, 8-12, 14-20, 22, 24-28, 30-34, 36, 37, and 39.

The Applicant amends claims 1, 11, 22, 24, 30, and 31. No new matter is added.

The application remains with claims 1, 2, 4-6, 8-12, 14-20, 22, 24-28, 30-34, 36, 37, and 39 after entering this amendment.

Claim Rejections - 35 U.S.C. § 103

The Examiner rejected claims 1, 2, 4-6, 8-12, 14-16, 18-20, 22, 24-26, 28, 30-34, 36, 37, and 39 under 35 U.S.C. § 103(a) over Cowie *et al.* (U.S. Patent Application Publication No. 2003/0023865) and variously in view of Feigen et al. (U.S. Patent Application Publication No. 2002/0138554), Pierre Richer: SANS/GIAC Practical Assignment for GSEC Certification Version 1.4b: Steganalysis: Detecting hidden information with computer forensic analysis, SANS Institute 2003 ("Richer"), and/or Charbonneau (U.S. Patent No. 7,526,654).

Whereas the rejection is traversed, Applicant amends claims 1, 11, 22, 24, 30, and 31 only to expedite prosecution, and without prejudice to pursuing the claims as previously presented or in other forms in a continuation or other application. For example, amended claim 1 recites a method, comprising:

> locating a steganographic program comprising executable code that includes software calls that introduce steganographic items into a computer file;
>
> obtaining a steganographic signature by reading a partial section of the executable code;
>
> identifying, with a processing device, computer files comprising software code, wherein the steganographic program is excluded from the identified computer files;
>
> obtaining one or more test signatures by reading partial sections of the software code;
>
> comparing the steganographic signature with the one or more test signatures; and
>
> displaying, based on said comparing, a listing of which of the computer files comprise software code that has been modified by the steganographic program.

Cowie is directed to a system of detecting computer programs where fingerprint data indicative of predetermined characteristics of resource data are used to compare the suspect file with a library of Trojans and worms (paragraph 0012). In rejecting claim 1, the Examiner stated that Cowie fails to disclose "that the code read is executable code or that partial sections of the

software code are read" and instead alleged that the newly cited reference "Feigen does teach these features" (page 3, first full paragraph of the June 15, 2011 Office Action).

Even assuming, for argument's sake, that Feigen's copy of the code and/or hash discloses a partial section of executable code, Applicant respectfully submits that the combination of Cowie with the Feigen reference nevertheless still fails to disclose the recited features. According to Cowie, the "invention relates to the detection of known computer programs within packed computer files" (par. 0002). The known computer programs include "known Trojans or worms" (par. 0011) of a "suspect packed computer file" which are compared with "a library of fingerprint data of known computer programs" (par. 0012). In other words, Cowie is looking for instances of the known Trojans or worms in the packet computer files which match the same Trojans or worms in the library of known computer programs. Accordingly, Applicant respectfully submits that Cowie fails to disclose *identifying, with a processing device, computer files comprising software code, wherein the steganographic program is excluded from the identified computer files.*

Feigen is directed to a "method of verifying the integrity of software resident on a remote network appliance..." (Abstract) in order "to determine whether a remote device has been tampered with, for example, a user to obtain unauthorized access to paid programming" (par. 0002). According to Feigen, "the host performs a hash function on a copy of the code under inspection which is maintained by the host... (and the) host then transmits the hash function to the remote device whereupon the remote device performs the same hash function on the 'same' block of code resident in the remote device" (par. 0010).

Furthermore, according to Feigen, "If the two hash values match, the host concludes that the block of code resident in the remote device corresponds to the copy of that same block of code maintained by the host" (par. 0010). In other words, Feigen is comparing two copies of the same program, one copy at the remote device and one copy at the host, to determine if they match. It would be contrary to the stated purpose of Feigen to exclude the copy of the program at the remote device from the hash value comparison. Accordingly, Applicant respectfully submits that Feigen also fails to disclose *identifying, with a processing device, computer files comprising software code, wherein the steganographic program is excluded from the identified computer files.*

Additionally, in so far as both Cowie and Feigen are understood to be directed to looking for instances of a known program, Applicant respectfully submits that the proposed combination also fails to disclose *displaying, based on said comparing, a listing of which of the computer files comprise software code that has been modified by the steganographic program*, as recited by claim 1. Even if a worm or virus is located within packed computer files, as disclosed by Cowie, it is the worms or viruses, e.g., the "known computer programs," themselves that are being looked for (par. 0002), rather than any software code modified by Cowie's known computer programs.

At page 3 and continuing to page 4 of the June 15, 2011 Office Action, the Examiner alleged that it would be obvious to combine Cowie with Feigen "since this would increase the probability of detecting hidden malware in a file", and that the further incorporation of Richer would be obvious "since this would extend the types of programs that can be evaluated for embedded malware." Applicant respectfully disagrees.

The Supreme Court acknowledged the importance of identifying "a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements in the way the claimed new invention does" in an obviousness determination. *KSR*, 127 S. Ct. 1727 at 1731 (2007). Additionally, if one of the references 'teaches away' from the combination of references (i.e., teaches away from the missing claim element), it is strong evidence of non-obviousness.

As discussed above, Cowie and Feigen describe looking for instances of the same known program or a copy of the same program. In Cowie, the known programs in a library are compared with fingerprint data to determine if the known programs are also in the packed files, whereas Feigen describes comparing copies of the same program residing at the remote device and at the host. Accordingly, the proposed combination also teaches away from the recited features of *identifying, with a processing device, computer files comprising software code, wherein the steganographic program is excluded from the identified computer files*.

Whereas Cowie is directed to the detection of Trojans or worms and Feigen is directed to determining whether a remote device has been tampered with, Applicant further remarks that the Richer reference is directed to yet a different technological area of Steganalysis. Applicant respectfully submits that it would not be obvious to one of ordinary skill to combine the three rather disparate references in the manner proposed by the Examiner for similar reasons as discussed above.

Claims 11 and 31 are believed to be allowable over the cited art for similar reasons as claim 1. As claims 2, 4-6, 8-10, 12, 14-16, 18-20, 22, 24-26, 28, 30, 32-34, 36, 37, and 39 depend directly or indirectly from independent claims 1, 11, and/or 31, the comments and revisions directed above to claims 1, 11, and 31 apply equally to claims 2, 4-6, 8-10, 12, 14-16, 18-20, 22, 24-26, 28, 30, 32-34, 36, 37, and/or 39, respectively. In addition, claims 2, 4-6, 8-10, 12, 14-16, 18-20, 22, 24-26, 28, 30, 32-34, 36, 37, and 39 recite further subject matter. Accordingly, reconsideration and withdrawal of the rejection of claims 1, 2, 4-6, 8-12, 14-16, 18-20, 22, 24-26, 28, 30-34, 36, 37, and 39 is respectfully requested.

Applicant believes that the Examiner's reliance on Atkinson in rejecting claim 4 at page 9 of the June 16, 2011 Office Action appears to have been in error, and that the Examiner had intended to reference the newly cited reference to Feigen in place of Atkinson. Clarification is requested in the event that claim 4 continues to be rejected.

Allowable Subject Matter

The Examiner objected to claims 17 and 27 as being dependent upon a rejected base claim, but indicated that they would be allowable if rewritten in independent form, including all of the limitations of the base claim and any intervening claims.

While Applicant agrees with the Examiner that claims 17 and 27 are allowable, Applicant respectfully declines to amend claims 17 and 27 on the basis that the independent claims 11 and 31, upon which they depend, are themselves allowable as discussed above with respect to the 35 U.S.C. § 103 rejection.

Any statements made by the Examiner that are not addressed by the Applicant do not necessarily constitute agreement by the Applicant. In some cases, the Applicant may have amended or argued the independent claims thereby obviating grounds for rejection of the dependent claims.

CONCLUSION

For the foregoing reasons, the Applicant respectfully requests reconsideration and allowance of the present application. The Examiner is encouraged to telephone the undersigned at (503) 546-1812 if it appears that an interview would be helpful in advancing the case.

Customer No. 73552

Respectfully submitted,

STOLOWITZ FORD COWGER LLP

Bryan Kirkpatrick

Bryan D. Kirkpatrick
Reg. No. 53,135

STOLOWITZ FORD COWGER LLP
621 SW Morrison Street, Suite 600
Portland, OR 97205
Telephone: 503-224-2170
Fax: 503-224-2084
Email: docket@stofoco.com